SECURITY AWARENESS

OCTOBER 2001

Introduction

This newsletter focuses on security vulnerabilities and threats, as well as the measures GOT is taking to reduce and prevent them in continuing to provide secure network services.

Vulnerabilities

Hackers can get into our most important systems in minutes, sometimes-even seconds. Our environment is probed on a daily basis. We are involved in an ongoing effort to create a process of notification when new vulnerabilities are discovered.

GOT has seen many intrusions, and the main ones have been vulnerabilities from systems that have not been updated or patched. We have encouraged agencies to have a process in place ensuring that security patches are reviewed on a regular basis.

In this issue, we will focus on the following exploits:

1) Anonymous FTP Access
2) Folder/Directory/Traversal
3) "Code Red" Worm
4) "Nimda" Worm

Anonymous FTP Access is one of the most common vulnerabilities. There are multiple FTP servers within the Commonwealth's network that allow anonymous access. In some cases, servers running anonymous FTP have been used for purposes other than what was

Continued on page 2

INSIDE THIS ISSUE

Public Key Infrastructure

The Governor's Office for Technology (GOT) is implementing a Public Key Infrastructure (PKI) for the Commonwealth. PKI is a technology that enables many enhancements to a security framework, including encryption of sensitive data (confidentiality), digital electronic signatures (authentication and integrity), and absolute verification of the identity of the parties using the technology (non-repudiation). The services encompassed by PKI include secure e-mail, secure Electronic Data Interchange (EDI), secure electronic forms, secure desktops, reduced logon, secure remote access, and other services.

The initial PKI project for the Commonwealth will be limited to providing secure e-mail using the Express product from Entrust Technologies. The Entrust/ Express product enables users to seamlessly encrypt and digitally sign e-mail using Microsoft Outlook and Exchange. Encryption allows data to be transmitted by the sender in an undecipherable format over the network, granting only the recipients specified the ability to view the contents. Digital signatures provide proof that the sender was the originator of the data, and also that the content has not been altered or changed since the sender "signed" the data. The process also provides identity verification to ensure that only the sender could have originated the data that was sent.

3270 Encryption

GOT has been involved in a process to encrypt the 3270 client software log-in process by using an upgraded version of Attachmate's "Extra" software. This software allows the ability to talk to the mainframe from a personal computer. It is GOT's goal and objective to provide a secure infrastructure for those agencies that have a requirement to transmit UserIDs, passwords, and sensitive information across the network. GOT is working on a plan to provide both secure and unsecured Telnet connections to the OS390 server. It will be up to each agency to determine its own requirement, as to which environment they utilize in accessing their information.

intended. The FTP servers can have remote control programs installed which can be used to attack other machines. FTP servers with anonymous access can be used as intermediary storage locations by hackers, and most certainly the information stored is either illegal or belongs to someone else. Therefore, strict control over FTP servers is necessary.

The Folder/Directory/Traversal exploit refers to a security vulnerability existing in Internet Information Services (IIS) versions 4.0 and 5.0. This type of exploit allows a malicious user to gain access to files and folders which are located on the logical drive. This exploit also allows the prober the potential of taking a wide range of destructive actions against the network, one in which includes illegally running programs on a server which is restricted to Commonwealth use.

On Thursday, July 19, 2001, the state network was hit with a large attack of the "Code Red" worm. "Code Red" is a self propagating malicious code which randomly infects unpatched IIS indexing servers. Although the main target of the worm was Microsoft IIS web servers, the worm has also had the side affect of causing problems with printers that have a web management interface. While it has been confirmed that Lexmark printers were affected, it remains possible that **ANY** web manageable printer may have been affected.

Approximately 9:00 AM Tuesday, September 18, 2001 the Governor's Office for Technology experienced a disruption of network services due to a new software worm, W32.Nimda.A@mm. Collateral damage from Nimda includes network performance degradation due to high consumption of bandwidth during the propagation process. Nimda is a mass mailing worm that utilizes multiple methods to spread itself. The virus has several distinct propagation methods:

- Unpatched Microsoft IIS Servers;
- Known NT vulnerabilities;
- As an e-mail attachment; (README.EXE)
- As an e-mail message preview;
- By visiting an infected internet site;
- Sending e-mail through unauthorized systems;
- Through modifying registry settings in order to create open shares;
- Through reactivation of a guest account and making it a member of the administrator's group;
- An active attack using one of sixteen known Microsoft Web Server Holes.

Password Security

GOT's Division of Security Services will be regularly reviewing password practices of those utilizing its mainframe and networks servers.

To increase awareness of password security and to ensure compliance with policy GOT-067-2.1 (Section 3.3 - Password Length/Composition), GOT has implemented proactive password assessments. Once a month, GOT attempts to "crack passwords" in an attempt to discover weaknesses before an attacker.

In addition to this, several password cracking tools have been procured. These tools will be run on a regular basis.

The first RACF audit determined that many UserIDs needed to be strengthened. GOT staff met with agencies to review the lists and encouraged them to strengthen their passwords.

GOT is in the process of scheduling for implementation of the mandatory eight-character mainframe password that was identified in the Crowe Chizek audit (see "Auditing" on page 4). This modification will be implemented via GOT's change control process.

Workstation Security

GOT's workstation security policy GOT-067-1.5 (Section 2.5 – Unattended Workstation Processing), states that workstations should not be left unattended. Workstation audits at GOT facilities will occur in the immediate future. Most recently, an audit was conducted at the Cold Harbor facility. A notice was left at those workstations that had been left unattended. In order to ensure that you abide by this policy, the following instructions detail how to automatically have the screen saver lock the workstation:

- Right click anywhere on the desktop.
- Click "properties" to display the "Display Properties" dialog box below (or Control Panel/Display), and click the "Screen Saver" tab.
- Click the "password protected" box under the "Screen Saver" settings, and select the number of minutes you desire.
- Click the OK button.

Firewalls

Firewalls help provide a line of defense between a trusted network and a non-trusted network. This line of delineation is usually between the Internet and the Intranet. However, firewalls can be distributed throughout a network for added security for the following:

- Specific networks
- Server farms
- Extranet connections

A firewall's primary purpose is to force all traffic entering or leaving a network to pass through it, so the traffic can be checked to see that it is acceptable. When a firewall supports many different customers, it is important to have all parties work together for a firewall policy that can be supported and enforced to reduce risk for everyone.

Firewalls are the foundation on which security plans are built. However, they are not completely protected from attacks that are a direct result from unacceptable traffic which has found a way to gain access into a network. An example would be if http or web traffic were allowed to enter internal networks behind the firewall. The firewall would have to pass the traffic to its destination address (this could include hackers who are probing the network looking for security weaknesses). This is why demilitarized zones (DMZ) were established on firewalls. This helps to reduce risk by placing all devices that need Internet visibility on a network, separate from the Intranet, so that the traffic could then be closely monitored by additional security products such as:

- Network based intrusion detection systems (IDS)
- Host based IDS

In addition, firewalls cannot protect from malicious employees on the inside. While a firewall can block certain outbound connections, a malicious or disgruntled employee can harm an organization in other ways. Some examples are as follows:

- Copying sensitive data to disk, tape, or paper;
- Risking the allowance of continual connection to networks infected with trojans, worms, and viruses;
- Maintaining external connections such as DSL, or modems connected to other Internet Service Providers (ISPs);
- Hosting game servers on company resources, which can also allow a trojan, worm, or virus in;
- Participating in Internet file sharing systems such as Napster;

The state approved standard for firewall services is Firewall-1 by Checkpoint. More information can be found at: http://www.state.ky.us/ftp/pdf/2000_0201.pdf.

Virtual Private Networking

Virtual private networking (VPN) has emerged as the next big hit in security technology. VPN allows organizations to use a public network like the internet to connect to intranet resources, as if it were connected on the local area network (LAN).

All VPNs work fundamentally the same way. Their traffic is encrypted and encapsulated into new packets and transmitted to a device, usually a firewall running encryption software, that undoes the encapsulation; checks the integrity; and decrypts the traffic sending it to its destination.

VPNs allow organizations to use cheaper, shared networks such as cable modems, DSL, dialup accounts, or other broadband connections - opposed to dedicated leased line connections. Virtual networks also provide some additional security benefits.

A VPN tunnel conceals all the traffic that goes through it. Not only does it encrypt the traffic, but it also hides the identity of the internal resources being used, as well as the protocol it is communicating with. An example would be encrypted internet mail, anyone perusing the network would know mail is being sent since smtp is the protocol being used. With VPN, not only would the information be encrypted, but the protocol is hidden as well, due to the encrypted tunnel.

The ability to use any protocol with VPN is equally important. If a corporation prefers its users utilize Outlook to read mail from ISP accounts or other foreign connections, VPN can help secure the information and reduce exposure. This is done by providing the filtering of Microsoft Server Message Block (SMB) protocols which are needed to connect with the Exchange server.

VPN technology also holds some risk. Although the resource using the encrypted tunnel appears to be protected, the tunnel can be hijacked, resulting in an unauthorized user gaining access to the network or resources. This can be eliminated by deploying personal firewalls on remote computers and using host-based IDS programs. Any VPN tunnel allowed to be terminated inside of a network that is not centrally managed is also a risk, because this bypasses all security platforms. Departments with extended VPN needs should work with their Security Division to create a specialized VPN deployment, ensuring that the corporation's security objectives are not compromised.

Virtual private networks are becoming more popular. VPNs have become a much-needed technology because of increased broadband services. This increases employee productivity. The state's standard for VPN services is VPN-1 by Checkpoint, which integrates the firewall platform for a total security suite.

Auditing

GOT is audited annually as part of the state's financial system's revenue process. This audit is called SAS-70, which is under the responsibility of the State Auditor's office. Crowe Chizek is the current vendor on contract with the Auditor's office to perform this service. The most recent audit began in June and was performed during the weeks of June 11 and June 25. GOT controls were tested to ensure sufficiency in providing a secure network. Although multiple areas were tested, examples of control areas included disaster recovery, physical security, and mainframe security (RACF). Examples of infrastructure controls included firewalls, VPN, IDS, and virus protection.

Tips for Web Servers

Public Servers are very attractive targets for attackers because of the public exposure. Most web attackers will attempt to vandalize the home page with inappropriate words and images. When they succeed, they post the "trophy" on a mirror site. These sites provide a "shopping list" for other attackers and put the web server at greater risk. It is pertinent to provide a high level of security before a web server is deployed.

The following steps are considered "best practices:"

- Stay up to date on security patches by subscribing to vendor security mailing lists. Apply security patches appropriately.
- Secure the host operating system.
- Dedicate the web server for web services only and minimize functionality.
- Maintain, review, and back up audit logs daily.
- Install web server software on separate physical disk partition.
- Display an acceptable use policy.

The following sites are excellent sources of information for security administrators, as well:

http://www.sans.org

http://www.nipc.gov/warnings/computertips.htm

http://www.cert.org

http://www.nipc.gov

http://www.securityfocus.com

http://www.state.ky.us/got/ois/security/security.htm

Disaster Recovery Test

On May 11-13, 2001, GOT managed a disaster recovery test for selected critical systems. The test was conducted within a 48-hour window through Sungard Recovery Service's site in Philadelphia, Pennsylvania, and a consolidated user site located at the Commonwealth Data Center. Sungard has been under contract with GOT since 1997 to provide on-going disaster recovery services, which includes annual test time.

This procedure included, for the first time, the recovery and testing of a server with a UNIX operating system. The following cabinets participated in the test:

- Finance
- Transportation
- Families and Children Cabinets

Systems tested included:

- MARS Advantage and Brass subsystems
- KAMES
- KASES
- Transportation Payroll
- Automated Licensing and Taxation
- U-Drive-It

GOT provided systems support for the mainframe (OS390) at both the Sungard and Commonwealth sites, and for the UNIX environment at the Sungard site. GOT also provided testing personnel for the MARS Brass subsystem. Verification of the results indicated that the tests were successful.

Anti-Virus Protection

GOT realizes that using a tiered approach to anti-virus protection is the best way to defend its network against viruses, worms, and trojans. GOT has an agreement with McAfee of Network Associates for anti-virus protection and uses the following McAfee products: 1) VirusScan on the desktops, 2) Netshield on the file, application, print, and web servers, and 3) GroupShield on the e-mail servers.

And just recently, GOT added another tier to provide anti-virus protection for a large portion of the state's Internet mail. WebShield has been implemented to provide security against e-mail viruses arriving from outside the state government's e-mail system. E-mail coming from the Internet gets scanned for viruses by WebShield before it is allowed to enter the state government's network.

As mentioned earlier, each of GOT's e-mail servers has its own anti-virus software (GroupShield) that ensures viruses cannot be delivered to or sent from that e-mail server. However, WebShield extends the reach of anti-virus protection by prohibiting Internet viruses from ever getting delivered to a mail server. Presently, WebShield scans on average approximately 100,000 messages per day that arrive from the Internet. The present rate of infection for Internet mail is about .2 percent (2 in every 1,000 messages), so on an average day, about 200 messages arriving from the Internet will contain viruses.

As viruses get more sophisticated and encryption becomes more than just a luxury in the workplace, agencies need to adapt their defences. One type of security or one level of anti-virus protection simply isn't enough. It is essential that each user has updated anti-virus software on their desktop as the first level of anti-virus defense, and that the software is configured to get the latest DATs and engines on a timely basis. GOT is taking this measure as well as doing everything possible to be sure that other bases are covered by protecting the gateway, protecting the servers, and thus protecting the users. Please see the anti-virus policy at http://www.state.ky.us/got/ois/security/antivirus/avpolicy.htm